

Análisis de las herramientas digitales para el seguimiento del COVID-19 de la Alcaldía de Bogotá

Este informe se basa en investigaciones que se hicieron principalmente entre el 29 de abril y el 20 de mayo del 2020 para los formularios "Bogotá Salud Capital" y a inicio de junio para la plataforma "Bogotá Cuidadora" y su aplicación GABO. Algunos complementos en itálica mencionan cambios que se hicieron desde los primeros análisis.

Sin embargo, ya que las herramientas digitales implementadas en el marco de la epidemia cambian constantemente, algunas de las conclusiones de este informe podrían ya no ser vigenten a la fecha de su publicación.





1. Descripción y metodología del análisis

El presente documento presenta los resultados de los análisis que hizo el laboratorio de seguridad digital y privacidad de la Fundación Karisma (K+Lab) de los formularios web "Bogotá Salud Capital" implementados por la Secretaría Distrital de Salud de Bogotá, en el marco de la epidemia de COVID-19 (parte 2), y más recientemente de la plataforma web *"Bogotá Cuidadora"* y su aplicación asociada *GABO* (parte 3). Por último se contemplan las problemáticas asociadas al uso de herramientas de publicidad dirigida para alertas de COVID-19 que se vinculan con el formulario "alerta" de *Bogota Salud Capital* (parte 4).

Nuestro análisis se enfocó en revisar los elementos de transparencia e información, privacidad y seguridad digital. Los resultados se presentan de forma sintética en dos tablas y son soportados con elementos técnicos que aparecen en el anexo.

Este análisis puso a la luz una vulnerabilidad de seguridad digital vinculada con el envió de datos personales de estos formularios de forma insegura (vía el protocolo HTTP). Se encontraron también vulnerabilidades de impacto moderado. Finalmente, varios elementos (uso de la herramienta de notificación True Push, reporte de movilidad, uso de publicidad y rastreo en el contexto del COVID-19) generan problemáticas de privacidad importantes, a pesar algunas de mejoras recientes que se pudieron apreciar.

El objetivo de este trabajo es el de contribuir al mejoramiento de la seguridad digital, privacidad, transparencia e información pública. La metodología que usamos se basa en análisis técnicos externos y no intrusivos. Se evaluó la información pública, el código fuente de la página web (HTML/javascript), las cookies y los rastreadores, permisos de la app y los flujos/paquetes de datos generados al completar y enviar los formularios. Para esto, se usaron las siguientes herramientas de código abierto:

- los navegadores *Mozilla/Firefox*, *Waterfox*[1];
- la extensiones de navegador *Cookie Manager* + (visualización de las cookies y sus características)[2] y *Wappalyzer* (análisis de las tecnologías de un sitio web)[3];
- la herramienta *Exodus Privacy*[4] (análisis estático de los permisos y rastreadores de una app);

1 Waterfox (https://www.waterfox.net/) es un navegador derivado de Mozilla/Firefox, de código abierto (Mozilla Public License, version 2.0). Permite un alto nivel de configuración y de compatibilidad con las extensiones

2 https://github.com/vanowm/FirefoxCookiesManagerPlus

3 https://www.wappalyzer.com/download

4 https://exodus-privacy.eu.org/





- las herramienta de captura de flujos/paquetes HTTP(S): OWASP ZAP[5] y Wireshark[6].

Antes de realizar los análisis envíamos un correo electrónico a la Secretaria de Salud de Bogotá informando de este ejercicio [ver Anexo 0].

5 https://www.zaproxy.org/ Es necesario mencionar que esta herramienta se usó exclusivamente en “modo seguro” de tal manera que se hicieran sólo análisis no intrusivos, del lado del cliente (de nuestro computador), analizando los flujos de datos saliendo y entrando de nuestro navegador.

6 https://www.wireshark.org/





2. Tabla sintética del análisis de los formularios “Bogotá Salud Capital”

Categoría	Formulario COVID-19 “Alerta”	Formulario Habitos / Autocuidado	Formulario Resultados exámenes
URL y alojamiento del servidor web	http://tramitesenlinea.saludcapital.gov.co/covid-19/ @IP: 208.30.40.188 (ETB Cololombia)	http://tramitesenlinea.saludcapital.gov.co/covid-19/habitos/ @IP: 208.30.40.188 (ETB Cololombia)	http://covid19.saludcapital.gov.co/resultados @IP: 190.27.239.122 (SECRETARIA DISTRITAL DE SALUD)
Información / Política de datos	Es necesario aceptar una autorización de tratamiento de datos personales antes de diligenciar el formulario (ver Anexo 1). Este texto mencioná que la “*Secretaría Distrital de Salud actuará como Responsable del Tratamiento de datos personales*” y que la finalidad del tratamiento es el “*análisis de información, seguimiento individual ante la situación de salud y acciones de salud pública que se requieran en el marco de la pandemia por COVID-19*”. Menciona los derechos de los usuarios y hace referencia a la política de tratamiento de datos personales de la Secretaría distrital de Salud y del Fondo Financiero de Salud[7].		En el pie de página, hay un enlace a la política de tratamiento de datos de la Secretaría de Salud de Salud de Bogotá y del Fondo Financiero de Salud.
Datos personales colectados	- No. de identificación - Nombre - Correo electrónico - Teléfono - Dirección - EPS - Fecha de nacimiento - ¿Ha recibido un mensaje en el que se le alerta porque pudo estar en contacto estrecho con una persona que tiene coronavirus?	Auto-cuidado individual: - Idem formulario alerta - Cuestiones de autocuidado (higiene, evita contactos, uso tapaboca en caso de gripa, etc.) Auto-cuidado colectivo: - Idem formulario alerta menos EPS y fecha de nacimiento Seguimiento reporte: → Entregando sólo el No. de	- No. de identificación - Celular + Verificación con un código enviado por SMS hacia el celular

[7] http://www.saludcapital.gov.co/Documents/Politica_Proteccion_Datos_P.pdf

		identificación se puede acceder al reporte asociado al nombre y No. de identificación.	
Categoría	**Formulario COVID-19 “Alerta”**	**Formulario Habitos / Autocuidado**	**Formulario Resultados exámenes**
Certificado SSL/TLS y HTTPS	**NO** Las páginas usan el protocolo inseguro HTTP, lo que no permite validar la identidad del dominio, transmite los datos en una forma insegura y genera una alerta de seguridad en el navegador [ver Anexo 2]. Para el caso particular del formulario de resultados, aunque la página del formulario tiene una URL de tipo HTTP, lo que no permite al usuario tener confianza en la página, los datos del formulario se envían con el protocolo HTTPS y existe por lo tanto un certificado SSL [Ver línea siguiente y Anexo 4].		
Envió de datos del formularios	**Tanto el análisis del código fuente (HTML) cómo el análisis de flujo/paquetes muestran que el envío de datos se hace en un forma no cifrada, mediante el protocolo inseguro HTTP [ver Anexo 3].**		**En el formulario de resultados, los datos se envían con el protocolo seguro HTTPS a pesar de que la página tiene una URL de tipo “http://”. [Ver Anexo 4]**
Rastreadores y cookies de terceros	- Servicio de analítica de datos de Google (Google Analytics, cookies *_ga* y *_gid*)	- Servicio de analítica de datos de Google (Google Analytics, cookies _ga y _gid) - Servicio externo de notificaciones TruePush (cookies *tp* y *sesionId*) Ambos servicios tienen un impacto negativo en la privacidad de las personas usuarias ya que las visitas e interacciones en estas páginas se transmiten a estas empresas que las pueden usar con fines publicitarios, directamente en el caso de Google e indirectamente en el caso de True Push[8], que puede compartir los datos con aliados publicitarios[9]. Se indica adicionalmente que las *cookies* de TruePush, que se instalan incluso si la persona no acepta el servicio de notificaciones, tienen una	

8 https://www.truepush.com/

9 Extracto de la política de privacidad de TruePush: “*In addition, cookies placed on your computer or your customer’s computer help us to understand what you or your customers are interested in. We or our ad-service platform may deploy online cookies to tracks users across websites or to associate users (and these cookies) with Mobile IDs We may do so in order to better or more accurately target relevant and contextual ads to you Our ad-serving platform may then help us retarget ads to your customers based on their interactions with Truepush.*”, https://www.truepush.com/privacy-policy





		duración de vida muy larga de 10 años[10] [Ver Anexo 6]. Resaltamos además que el servicio permite hacer notificaciones con una segmentación por localización entre otras. https://www.truepush.com/blog/why-truepush-is-free/	
Otros servicios externos	- Servicio de cartografía Arcgis - Otros servicios		
Versiones del servidor y herramientas web (actualizaciones)	- Servidor web *Apache 2.4.18* - El gestor de contenido *Code Igniter* - Frame work *Bootstrap 4.4.1* La versión del servidor Apache no es reciente (diciembre 2015[11]). Se han documentado ya varias potenciales vulnerabilidades en esta versión[12]. Además hay que resaltar que el servidor web divulga su versión detallada en sus respuestas HTTP, lo que no es recomendable puesto que podría dar información a un posible atacante y de esta manera se facilita un ataque.		- *Apache 2.4.29* - *Bootstrap 4.4.1* - *Code Igniter* La versión del servidor Apache no es reciente (octubre 2017). Se han documentado ya varias potenciales vulnerabilidades en esta versión.
Divulgación de errores de aplicación por el servidor		El servidor divulga errores del nivel aplicativo (PHP). En ciertos casos lo hace de manera aparente para el usuario y en otros en sus respuestas. Esto revela información técnica que podría ser usada por un atacante [Ver Anexo 7].	
Otras vulnerabilidades	El análisis con la herramienta *OWASP ZAP* mostró algunos problemas leves o moderados. Sólo queremos mencionar la ausencia de protección aparente contra los ataques de tipo “clickjacking”, debido a la ausencia de encabezado “X-Frame-Options” y de definición de “Content Security Policy” (CSP)[13].		

En cuanto a las vulnerabilidades, debemos resaltar que nuestro análisis es pasivo y no intrusivo. Por lo tanto, de hacer un análisis más profundo de tipo “pentesting” o una auditoría interna, probablemente se encontrarían otros problemas.

---

10 La *cookie* de tercerro “sessionId” del dominio “truepush.com”, a pesar de lo que podría dejar pensar su nombre, no es una *cookie* de sesión. Al contrario, tiene una duración de vida muy larga, de 10 años (fecha de expiración al 20 de marzo de 2030 en nuestro experimento) y contiene un número de identificación único (al formato hexadecimal). Por esto tiene todas las características de una *cookie* de rastreo.

11 https://archive.apache.org/dist/httpd/

12 https://httpd.apache.org/security/vulnerabilities_24.html

13 https://owasp.org/www-community/attacks/Clickjacking

Finalmente, hay que mencionar que se observaron tanto en resultados de búsqueda de Google cómo en Instagram publicidad en forma de alertas que apuntan hacia el primer formulario analizado en esta tabla. Esto deja más interrogantes en el uso de herramientas cómo TruePush, que se puede conectar con herramientas publicitarias. Este tema se detalla en la parte 4 de este documento .

Nota: al momento de redactar este informe aparece una plataforma que permite "de forma ágil y sencilla, usted tiene acceso a su historia clínica, agendamiento de citas y gestión de fórmulas médicas. ". Esta ubicada en la URL "https://ciudadanobogotadigital.saludcapital.gov.co/" e implementa el protocolo HTTPS.

3. Complemento sobre “Bogota Cuidadora” y la app GABO

<u>Nota previa</u>: Bogotá Cuidadora y la app Gabo se publicaron recientemente incorporando elementos de respuesta al Covid, de modo que en este análisis se hace una evaluación parcial que no puede considerarse revisión a todo el sistema desarrollado. Adicionalmente, deberá considerarse que al momento de finalizar este informe la aplicación GABO ya no esta disponible en la tienda de aplicaciones de Android (Play Store)[14]. Sin embargo todavía funciona y sus servidores responden.

La plataforma web “Bogota Cuidadora” y su aplicación asociada GABO, lanzada el 31 de mayo, tiene - además de una parte informativa - cinco componentes de finalidades muy distintas vínculadas con el COVID-19:

- “Necesito apoyo”: para solicitar apoyos de varios tipos (económicos, apoyo en servicios públicos, aplazar pagos de impuestos, etc.);
- “Reportar movilidad”: para hacer un reporte a la Alcaldía en caso de desplazamiento;
- “Reportar estado de salud”: para reportar su estado de salud y analizar los riesgos de ser contagiado con COVID-19;
- “COVID-19 a mi alrededor”: que provee un “Mapa de calor COVID-19”;
- “Ofrezco ayuda”: para ofrecer donaciones o ayudas, en conexión con la Red de cuidado ciudadano (https://reddecuidadociudadano.gov.co/) y el Instituto Distrtital de Participación y Acción Comunal (IDPAC) de la Alcaldía de Bogota.

Como ya se mencionó tan solo se analizan algunos componentes de esta plataforma. Este análisis es sintético y enfocado en el reporte de movilidad ya que al inicio era obligatorio para todas las categorías de desplazamiento lo que creaba un desafío especial en terminos de privacidad.

---

[14] La aplicación tenía como identificador “com.supercade” y se podía descargar en el Play Store en el enlace https://play.google.com/store/apps/details?id=com.supercade&hl=es_CO que ya no funciona.

Categoría	Formularios "Bogota cuidadora" (Reporte de Movilidad)	Aplicación "GABO" ("Bogota Cuidadora")
URL/dominio y alojamiento del servidor web	https://bogota.gov.co/bogota-cuidadora/ @IP: 20.36.244.102 y 13.107.6.194 (registro de movilidad en Microsoft Form) (Microsoft Corporation, Estados Unidos)	La aplicación se comunica principalmente con el dominio "api.bogota.gov.co" @IP: 104.209.235.43 (Microsoft Corporation, Estados Unidos)
Datos personales colectados **e** **Información**	• Nombre y apellido • Correo electrónico • Celular • Número de identificación • Fecha de nacimiento (para la app) • Localidad y dirección de residencia • Razón del desplazamiento • Hora de salida • Localidad y dirección de destino • Hora de llegada al destino El sitio web y GABO App cuentan con una política de privacidad de 11 páginas que no se analiza en esta evaluación puesto que ya se anunciaron revisiones de las autoridades correspondientes.	
Cifrado (HTTPS)	Tanto la aplicación cómo el formulario usan el protocolo cifrado HTTPS para transmitir los datos. Mostramos la captura de flujo correspondiente (ver Anexo 8).	
Rastreo y cookies		Además de las cookies funcionales, el uso de Microsoft Forms tiene cómo consecuencia la instalación de varias cookies de rastreo con duración de vida superior a un año, asociadas a los dominios "office.com", "microsoft.com" y "bing.com". En particular se puede mencionar la cookie de rastreo publicitario "MUID" de Microsoft Advertising, la filial publicitaria de Microsoft[15] (ver Anexo 9).
Supresión de datos		La página web integró hace poco un enlace que permite hacer una solicitud de supresión de datos personales para los registros de movilidad vía un formulario web[16].

15 https://about.ads.microsoft.com/en-gb/resources/policies/microsoft-advertising-click-measurement-description-of-methodology

16 https://forms.office.com/Pages/ResponsePage.aspx?id=y6dR80r58E2WJ64DDM73xAWOsPtqgIVEoXd0yQmVorxUQ1FRN0hZS1JMNUhIWjNKTEc2Q0hXV09ERC4u





4. Notificación de exposición por medio de publicidad en Facebook y Google.

En el transucurso de las últimas semanas hemos observado el uso de publicidad digital por parte de la Alcaldía de Bogotá en un formato que simula notificaciones de exposición al virus. Estos anuncios están enlazados con un formulario en la página de la Alcaldía donde se recopilan datos personales de las personas usuarias y se les indaga por síntomas relacionadas con la enfermedad Covid-19 (Formulario "Alerta", analizado en la parte 2).

En el Anexo 10 de este documento se encontran las capturas de pantalla para los anuncios en Google e Instagram relacionados con esta campaña.

El uso de tecnologías digitales para apoyar el proceso de rastreo de contacto, una medida de vigilancia de la salud afianzada en las estrategias de salud pública, es una área de reciente desarrollo donde se están haciendo ensayos que requieren particular cuidado. Recientemente la Organización Mundial de la Salud (OMS) publicó su guía "Consideraciones éticas para guiar el uso de tecnologías de rastreo de proximidad digitales para el el rastreo de contacto de la Covid 19"[17]. Uno de los propósitos de usar la tecnología es poder entregar alertas a quienes pudieron estar cerca de una persona que ha sido confirmada como positiva por Covid 19 para que se tomen medidas preventivas que incluyen el testeo y cuarentena. Ahora bien, este desarrollo no solo exige importantes consideraciones éticas, ya que puede poner en peligro derechos fundamentales, sino que además el debate internacional sobre cómo debe hacerse, su alcance y detalles incluso vinculados a cómo debe ser y quién puede recibir una alerta de este tipo, son discusiones claves que hablan de la efectividad e incluso posible medición de los resultados que darán luz sobre la efectividad del despliegue de estas soluciones.

El uso que se hace en Bogotá de publicidad en línea para simular procesos de rastreo digital de proximidad brinda una apariencia de uso de una medida de salud pública internacional que es obligatoria y que en esta práctica resulta simulada. Consideramos que esta práctica supone múltiples preocupaciones que están en proceso de análisis por Karisma. Mientras tanto, en este documento resaltamos las preocupaciones que se derivan de la simulación tecnológica que el distrito hace sin pudor, para generar una reflexión.

En relación con esta práctiva resaltamos los siguientes posibles problemas e incompatibilidades con las políticas de Google y Facebook:

- Pueden promover prácticas discriminatoras basadas en la condición médica de una persona.[18]

---

17 https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf

18 https://www.facebook.com/policies/ads/prohibited_content/discriminatory_practices





- Hace uso de atributos personales al determinar que por la ubicación una persosa puede estar infectada de coronavirus.[19]
- los anuncios implican que el anunciante posee información sensible e identificable de quien recibe el anuncio.[20]
- Es improbable que el algoritmo de despliegue de anuncios de Facebbok y de Google sea el apropiado para servir de "alerta" de sistemas de *notificación de exposición* ya que este sistema no parece estar basado en ninguno de los estandares conocidos para esta función[21].

Para Karisma el uso de este sistema al no estar vinculado al procedimiento de rastreo de contacto es ilegítimo, desproporcionado y no parece apropiado para el propósito de *notificación de exposición* ni sus estándares internacionales. Queremos resaltar que a pesar de la ausencia de documentos que expliquen lo que el distrito hace consideramos que ni siquiera se evaluó su efectividad, que no se consideró el índice de falsos positivos y falsos negativos que genera, ni la forma como esto puede acelerar el "cansancio" de alertas que ya acusan otras sociedades sin que en Colombia se haya desplegado siquiera este apoyo tecnológico. La emergencia sanitaria no justifica cualquier acción y mucho menos vinculada con medidas de salud públicas que se han construido con altos estándares científicos y dependen fuertemente de la confianza de las personas.

Un análisis a fondo de esta práctica está en curso al interior de Karisma. Nos encontramos consultando con empresas como Facebook y Google para ver el alcance de este desarrollo. Los resultados de ese análisis, una vez que no incluyen información de ninguna vulnerabilidad y que son de interés público, una vez completados serán publicados en nuestro sitio y difundidos a través de redes sociales. Para esta publicación esperamos contar con la explicación del Distrito sobre esta práctica en la que se incluya la respuesta a la siguiente pregunta: ¿Cúales son las bases teóricas para la aplicación de este procedimiento?

19 https://www.facebook.com/policies/ads/prohibited_content/personal_attributes
20 https://support.google.com/adspolicy/answer/143465?hl=en
21 https://web.karisma.org.co/aplicaciones-de-rastreo-digital-de-contactos-para-que-zapatos-si-no-hay-casa/





ANEXOS – Referencias

[0] Correo preliminar enviado a los encargados del sitio

Asunto: Análisis de los formularios web de la Secretaria de Salud de Bogotá
Fecha: Tue, 28 Apr 2020 17:22:09 -0500
De: XX - Karisma <XX@karisma.org.co>
Organización: Fundación Karisma
Para: contactenos@saludcapital.gov.co
CC: <XX@karisma.org.co>, <XX@karisma.org.co>

Buenas tardes,

La Fundación Karisma es una organización de la sociedad civil, fundada en 2003 y localizada en Bogotá, que busca responder a las oportunidades y amenazas que surgen en el contexto de la "tecnología para el desarrollo" para el ejercicio de los derechos humanos. Karisma trabaja desde el activismo con múltiples miradas —legales y tecnológicas— en coaliciones con socios locales, regionales e internacionales.
Desde hace varios años estamos evaluando aspectos de seguridad y privacidad de algunas páginas web y aplicaciones asociadas con trámites y servicios de interés público. Recientemente lo hicimos con la aplicación del Instituto Nacional de Salud "CoronApp". Estos análisis han sido de conocimiento del Ministerio de Tecnologías (MINTIC) que en varias ocasiones nos ha facilitado mecanismos de comunicación con los responsables de las plataformas evaluadas. Los análisis han llevado a mejoras de las plataformas. Esperamos que este sea nuevamente el caso.
En este momento estamos haciendo un análisis no intrusivo de los formularios del sitio web de la Secretaría de Salud de la Alcaldía de Bogotá ("saludcapital.gov.co") vinculados con la gestión de la epidemia actual en estos aspectos de privacidad y seguridad digital. Parte de nuestra evaluación incluye el análisis del tráfico de datos generado por los formularios que recopilan información personal. Por esto, queremos comunicarles que encontrarán registros a nombre de Karisma, asociados a correos con el dominio "@karisma.org.co". Estos datos no son reales y no deben ser tomados en cuenta para los reportes de salud ni la generación de alertas.
Una vez tengamos el informe de nuestros hallazgos los daremos a conocer en primera instancia a ustedes.
Si tienen alguna duda o inquietud sobre el tema pueden comunicarse con nosotros respondiendo este correo. Estaremos atentos a contestar cualquier pregunta.
Atentamente,

Fundación Karisma.





[1] Autorización de tratamiento de datos (al ingresar por primera vez)

AUTORIZACIÓN DE TRATAMIENTO DE DATOS PERSONALES

Dando cumplimiento a lo dispuesto en la Ley 1581 de 2012, "Por el cual se dictan disposiciones generales para la protección de datos personales" y de conformidad con lo señalado en el Decreto 1377 de 2013, con la aceptación de este documento manifiesto que he sido informado por La Secretaría Distrital de Salud (SDS) lo siguiente:

1. La Secretaría Distrital de Salud actuará como Responsable del Tratamiento de datos personales de los cuales soy titular y que, conjunta o separadamente podrá recolectar, usar y tratar mis datos personales conforme la Política de Tratamiento de Datos Personales de la SDS disponible en la página web de la entidad.

2. Que me ha sido informada la (s) finalidad (es) de la recolección de los datos personales, para análisis de información, seguimiento individual ante la situación de salud y acciones de salud pública que se requieran en el marco de la pandemia por COVID-19.

3. Se me ha informado que es de carácter facultativo o voluntario responder preguntas que versen sobre Datos Sensibles o sobre menores de edad.

4. Mis derechos como titular de los datos son los previstos en la Constitución y la ley, especialmente el derecho a conocer, actualizar, rectificar y suprimir mi información personal, así como el derecho a revocar el consentimiento otorgado para el tratamiento de datos personales.

5. Los derechos pueden ser ejercidos a través de los canales dispuestos por la SDS y observando su Política de Tratamiento de Datos Personales.

6. Mediante la página web de la entidad (www.saludcapital.gov.co), podré radicar cualquier tipo de requerimiento relacionado con el tratamiento de mis datos personales.

7. La SDS garantizará la confidencialidad, libertad, seguridad, veracidad, transparencia, acceso y circulación restringida de mis datos y se reservará el derecho de modificar su Política de Tratamiento de Datos Personales en cualquier momento. Cualquier cambio será informado y publicado oportunamente en la página web.

8. Teniendo en cuenta lo anterior, autorizo de manera voluntaria, previa, explícita, informada e inequívoca a la SDS para tratar mis datos personales de acuerdo con su Política de Tratamiento de Datos Personales para los fines relacionados con su objeto y en especial para fines legales, contractuales, misionales descritos en la Política de Tratamiento de Datos Personales y en la presente autorización.

9. La información obtenida para el Tratamiento de mis datos personales la he suministrado de forma voluntaria y es verídica.

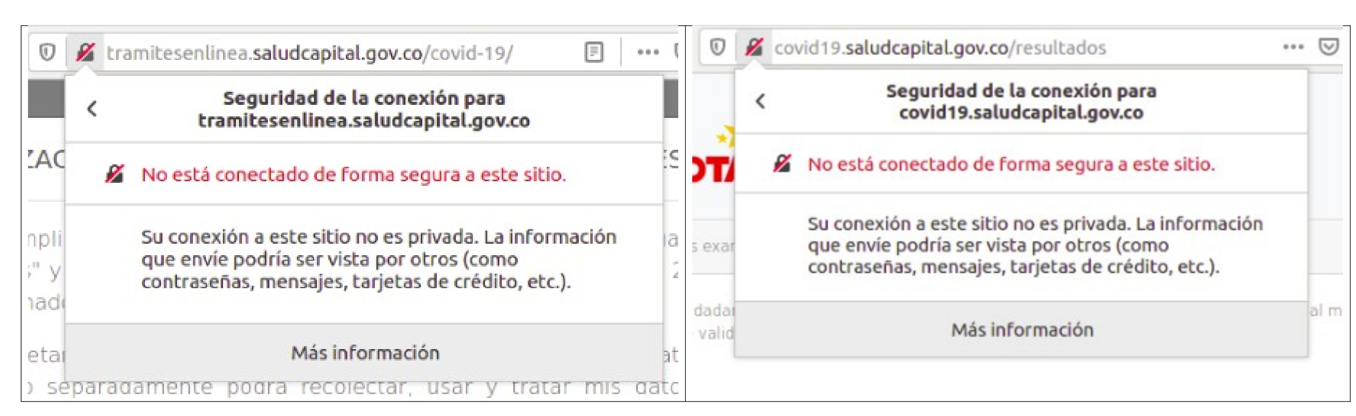
Acepto





[2] Uso del HTTP y alerta de seguridad

Los pantallazos siguientes, tomados en las páginas de formularios de los sub-dominios "tramitesenlinea.saludcapital.gov.co" y "covid19.saludcapital.gov.co" muestran el uso del protocolo inseguro HTTP y la alerta de seguridad que esto generó en nuestro navegador (aquí, Mozilla/Firefox).







[3] Envió de Datos a través de los formularios de forma insegura (HTTP, formularios Alerta y Autocuidado)

Aquí se muestran parte de los formularios de “Registro / Alerta” y de “Autocuidado” completados y de los flujos de datos correspondientes enviados por nuestro computador (OWASP ZAP). En ambos casos se envían con el protocolo HTTP y el método POST.

Diligencie los siguientes datos y preguntas. Luego, haga clic en Enviar

Número de identificación: 1234567891
Nombre: Fundacion Karismados
Correo Electrónico: test@karisma.org.co
Teléfono: 3124567890
Dirección: Transversal 22A#59-44
EPS: Sanitas
Fecha de Nacimiento: 01 - 01 - 1990

¿Ha recibido un mensaje en el que se le alerta porque pudo estar en contacto estrecho con una persona que tiene coronavirus?
Si / No

¿Tiene alguno de los siguientes síntomas?
Si / No

Fiebre cuantificada mayor o igual a 38°C
Tos
Dificultad para respirar
Dolor de garganta (Odinofagia)
Dolor de cabeza persistente
Fatiga/decaimiento o debilidad
Diarrea o vómito
Otros (trastornos neurológicos)

Inicio Rápido | Request & Response

Encabezamiento: Vista Raw | Cuerpo:Vista Raw

```
POST http://tramitesenlinea.saludcapital.gov.co/covid-19/covid/procesarForm HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-CL,es;q=0.8,en-US;q=0.5,en;q=0.3
Referer: https://tramitesenlinea.saludcapital.gov.co/covid-19/
Content-Type: multipart/form-data; boundary=---------------------------107231994397856855220439998858
Content-Length: 1800
Cookie: ci_session=bt5bdki8f163oo5j4t4k0sm3a855chpo; _ga=GA1.3.554872309.1589645666; _gid=GA1.3.
2072120160.1589645666
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: tramitesenlinea.saludcapital.gov.co

---------------------------107231994397856855220439998858
Content-Disposition: form-data; name="fechaTerminos"

2020-05-16 11:14:39
---------------------------107231994397856855220439998858
Content-Disposition: form-data; name="identificacion"

1234567891
---------------------------107231994397856855220439998858
Content-Disposition: form-data; name="nombre"

Fundacion Karismados
---------------------------107231994397856855220439998858
Content-Disposition: form-data; name="correo"

test@karisma.org.co
---------------------------107231994397856855220439998858
Content-Disposition: form-data; name="telefono"

3124567890
---------------------------107231994397856855220439998858
Content-Disposition: form-data; name="direccion"

Transversal 22A#59-44
---------------------------107231994397856855220439998858
Content-Disposition: form-data; name="eps"

Sanitas
```

REPORTE DE AUTOCUIDADO

Autocuidado individual | Autocuidado colectivo | Seguimiento reporte

Número de identificación: 1234567890
Nombre: Fundacion Karisma
Correo Electrónico: test@karisma.org.co
Teléfono: 3124567890
Celular: 3124567890
Dirección: Transversal 22A#59-44
EPS: Sanitas
Fecha de Nacimiento: 01 - 01 - 2000

Inicio Rápido | Request & Response

Encabezamiento: Vista Raw | Cuerpo:Vista Raw

```
POST http://tramitesenlinea.saludcapital.gov.co/covid-19/habitos/procesarFormInd HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-CL,es;q=0.8,en-US;q=0.5,en;q=0.3
Referer: https://tramitesenlinea.saludcapital.gov.co/covid-19/habitos/formHabitos
Content-Type: multipart/form-data; boundary=---------------------------51757126416618551635585186
Content-Length: 1931
Cookie: ci_session=3rdb6varup1h15ebt7lulqj9n58v0ejf; _ga=GA1.3.904515612.1589302730; _gid=GA1.3.
2075993712.1589302730
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Host: tramitesenlinea.saludcapital.gov.co

---------------------------51757126416618551635585186
Content-Disposition: form-data; name="identificacion"

1234567890
---------------------------51757126416618551635585186
Content-Disposition: form-data; name="nombre"

Fundacion Karisma
---------------------------51757126416618551635585186
Content-Disposition: form-data; name="correo"

test@karisma.org.co
---------------------------51757126416618551635585186
Content-Disposition: form-data; name="telefono"

3124567890
---------------------------51757126416618551635585186
Content-Disposition: form-data; name="celular"

3124567890
---------------------------51757126416618551635585186
```





Aquí se muestra – para el primero de estos formularios- un extracto de la captura hecha con el programa Wireshark que muestra igualmente el uso del protocolo inseguro HTTP (*Hyper Text Transfer Protol*) con el método POST y además muestra la dirección IP del servidor web destinatario (208.30.40.188, que pertenece a ETB Colombia).

```
› Frame 1814: 418 bytes on wire (3344 bits), 418 bytes captured (3344 bits) on interface 0
› Ethernet II, Src: klab-Inspiron-7559.local (84:ef:18:ce:6a:21), Dst: _gateway (70:5a:9e:46:da:3f)
› Internet Protocol Version 4, Src: klab-Inspiron-7559.local (192.168.0.16), Dst: 208.30.40.188 (208.30.40.188)
› Transmission Control Protocol, Src Port: 50253 (50253), Dst Port: http (80), Seq: 2108, Ack: 1, Len: 352
› [3 Reassembled TCP Segments (2459 bytes): #1812(659), #1813(1448), #1814(352)]
› Hypertext Transfer Protocol
˅ MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "--------------------------10723199
0330  2d 2d 2d 2d 2d 2d 2d 2d  2d 31 30 37 32 33 31 39   -------- -1072319
0340  39 34 33 39 37 38 35 36  38 35 35 32 32 30 34 33   94397856 85522043
0350  39 39 39 38 35 38 0d 0a  43 6f 6e 74 65 6e 74 2d   999858·· Content-
0360  44 69 73 70 6f 73 69 74  69 6f 6e 3a 20 66 6f 72   Disposit ion: for
0370  6d 2d 64 61 74 61 3b 20  6e 61 6d 65 3d 22 69 64   m-data;  name="id
0380  65 6e 74 69 66 69 63 61  63 69 6f 6e 22 0d 0a 0d   entifica cion"···
0390  0a 31 32 33 34 35 36 37  38 39 31 0d 0a 2d 2d 2d   ·1234567 891··---
03a0  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
03b0  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 31 30 37 32 33 31   -------- --107231
03c0  39 39 34 33 39 37 38 35  36 38 35 35 32 32 30 34   99439785 68552204
03d0  33 39 39 39 38 35 38 0d  0a 43 6f 6e 74 65 6e 74   3999858· ·Content
03e0  2d 44 69 73 70 6f 73 69  74 69 6f 6e 3a 20 66 6f   -Disposi tion: fo
03f0  72 6d 2d 64 61 74 61 3b  20 6e 61 6d 65 3d 22 6e   rm-data;  name="n
0400  6f 6d 62 72 65 22 0d 0a  0d 0a 46 75 6e 64 61 63   ombre"·· ··Fundac
0410  69 6f 6e 20 4b 61 72 69  73 6d 61 64 6f 73 0d 0a   ion Kari smados··
0420  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
0430  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 31 30 37   -------- -----107
0440  32 33 31 39 39 34 33 39  37 38 35 36 38 35 35 32   23199439 78568552
0450  32 30 34 33 39 39 39 38  35 38 0d 0a 43 6f 6e 74   20439998 58··Cont
0460  65 6e 74 2d 44 69 73 70  6f 73 69 74 69 6f 6e 3a   ent-Disp osition:
0470  20 66 6f 72 6d 2d 64 61  74 61 3b 20 6e 61 6d 65    form-da ta; name
0480  3d 22 63 6f 72 72 65 6f  22 0d 0a 0d 0a 74 65 73   ="correo "····tes
0490  74 40 6b 61 72 69 73 6d  61 2e 6f 72 67 2e 63 6f   t@karism a.org.co
04a0  0d 0a 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   ··------ --------
04b0  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 31   -------- -------1
04c0  30 37 32 33 31 39 39 34  33 39 37 38 35 36 38 35   07231994 39785685
04d0  35 32 32 30 34 33 39 39  39 38 35 38 0d 0a 43 6f   52204399 9858··Co
04e0  6e 74 65 6e 74 2d 44 69  73 70 6f 73 69 74 69 6f   ntent-Di spositio
04f0  6e 3a 20 66 6f 72 6d 2d  64 61 74 61 3b 20 6e 61   n: form- data; na
0500  6d 65 3d 22 74 65 6c 65  66 6f 6e 6f 22 0d 0a 0d   me="tele fono"···
0510  0a 33 31 32 34 35 36 37  38 39 30 0d 0a 2d 2d 2d   ·3124567 890··---
```

Este envió de datos por HTTP (POST) también se puede observar en el código fuente de las páginas web correspondiente a cada formulario:

- para el formulario "Alerta/Registro":
  `<form class="form" name="formContacto" id="formContacto" method="post" action="http://tramitesenlinea.saludcapital.gov.co/covid-19/covid/procesarForm" enctype="multipart/form-data">`

- para el formulario de "Autocuidado individual":
  `<form class="form" name="formContactoInd" id="formContactoInd" method="post" action="http://tramitesenlinea.saludcapital.gov.co/covid-19/habitos/procesarFormInd" enctype="multipart/form-data">`





[4] Envió de los datos con HTTPS en el formulario de resultados

El uso del protocolo HTTPS se observa en el código fuente HTML de la página web:

```
<form class="form" name="formResultados" id="formResultados" method="post" action="https://covid19.saludcapital.gov.co/index.php/resultados/consultar_usuario" enctype="multipart/form-data">
```

Y también en la captura HTTP(S):

https://covid19.saludcapital.gov.co/index.php/resultados/validar_codigo

POST /index.php/resultados/validar_codigo HTTP/1.1 **[solicitud -> servidor]**
Host: covid19.saludcapital.gov.co
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-CL,es;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: https://covid19.saludcapital.gov.co/index.php/resultados/consultar_usuario
Content-Type: multipart/form-data; boundary=---------------------------8199762591475339557424979679
Content-Length: 571
Cookie: ci_session=vvuviavmtsejh5dd7io026jddnoifipe; _ga=GA1.3.986954382.1589905795; _gid=GA1.3.1322833665.1589905795
Connection: keep-alive
Upgrade-Insecure-Requests: 1
-----------------------------8199762591475339557424979679: undefined
Content-Disposition: form-data; name="pid"
5b6312fa04de0aaa0e57198d0488523893e0731d
-----------------------------8199762591475339557424979679
Content-Disposition: form-data; **name="identificacion"**
74XXXX
-----------------------------8199762591475339557424979679
Content-Disposition: form-data; **name="celular"**
312XXXX
-----------------------------8199762591475339557424979679
Content-Disposition: form-data; **name="codigo"**
YM3GQA
-----------------------------8199762591475339557424979679--

HTTP/1.1 200 OK [respuesta del servidor web]
Date: Tue, 19 May 2020 17:50:11 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Cache-Control: public, must-revalidate, max-age=0
Pragma: public
Set-Cookie: ci_session=tdejdviifo66gfk1m4np0kmfpv0m5q3c; expires=Tue, 19-May-2020 19:50:11 GMT; Max-Age=7200; path=/; HttpOnly
Content-disposition: inline; filename="mpdf.pdf"





X-Generator: mPDF 8.0.5
Last-Modified: Tue, 19 May 2020 17:50:11 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/pdf

Aquí mostramos el archivo PDF de Resultados se análisis que envia el servidor en respuesta a la consulta (datos personales ocultados):



Secretaría Distrital de Salud
Laboratorio de Salud Pública
Area de VIGILANCIA DE ENFERMEDADES
Carrera 32 No. 12-81 Teléfono PBX 3649090
Extensiones 9938/9937/9928/9929

Informe Individual Vigilancia Virus Respiratorios [redacted]

Número de radicado: 2020-[redacted]

IDENTIFICACIÓN			
Institución Procedencia	IPS BEST HOME CARE - Av 28 69 76 To 3 Ps 12	**Nombre completo**	[redacted]
Identificación	[redacted]	**Fecha de recepción**	02/04/2020
Tipo muestra	HISOPADO NASOFARINGEO		

ANÁLISIS VE GENERAL

RESULTADO DEL ANALISIS GENERADO POR EL LABORATORIO DE SALUD PUBLICA

Resultado COVID-19 (rRT-PCR Virus SARS-CoV-2)

Método de Análisis	Corman, et. Al (2020-V2) Charité Virology, Berlin, Germany	**Fecha Generación de Reporte**	2020-05-19
Resultado NUEVO CORONAVIRUS SARS-CoV-2	Negativo para NUEVO CORONAVIRUS SARS-CoV-2		

El Laboratorio de Salud Pública se responsabiliza exclusivamente de los análisis practicados a la muestra recepcionada.
La información consignada en el resultado del ensayo, corresponde a la registrada en el acta de toma de muestra.
El informe no se debe reproducir sin aprobación previa del Laboratorio

Reporte de uso exclusivo para el ciudadano. Recuerde que esta información es parcial e informativa. Por favor acérquese a reclamar su resultado en la institución donde tomo la muestra

Nota: el test sobre este formulario (y sólo para este) se hizo con datos reales (aquí ocultados) de una persona a quien se le realizó la prueba, con su consentimiento para la realización de este análisis técnico.

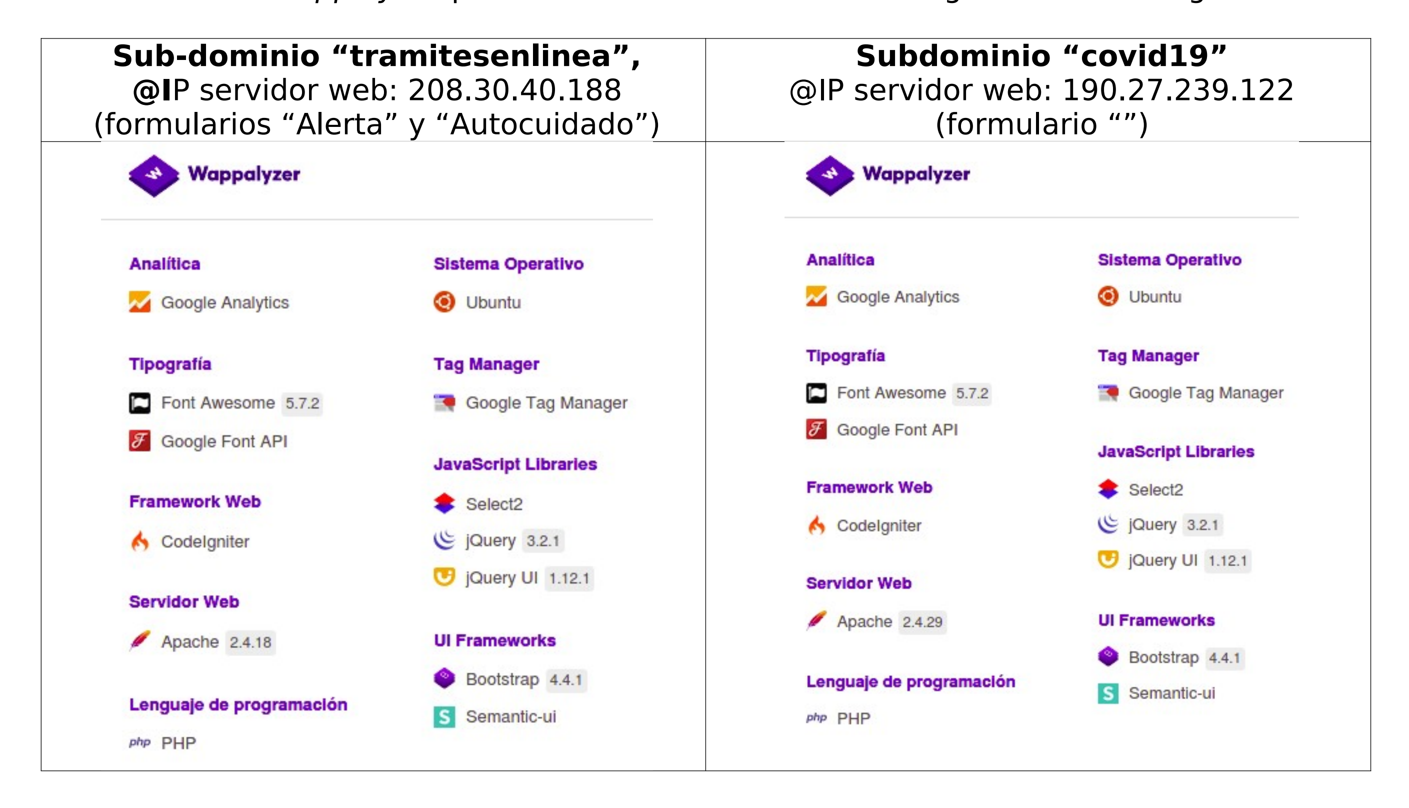




[5] Características de los servidores web y sus tecnologías

La herramienta *Wappalyzer* puso en evidencia el uso de las siguientes tecnologías

Sub-dominio "tramitesenlinea", @IP servidor web: 208.30.40.188 (formularios "Alerta" y "Autocuidado")	**Subdominio "covid19"** @IP servidor web: 190.27.239.122 (formulario "")



Se puede observar que tienen las mismas tecnologías en las mismas versiones (en aquellas en las que se puede observar), con excepción del servidor web Apache que tiene una versión más reciente en el segundo caso.

El uso de algunas de estas herramientas también aparece en los flujos de datos y la versión de los servidores web se muestra en sus respuestas HTTP de esta forma:

```
HTTP/1.1 200 OK [subdominio "tramitesenlinea"]
Date: Tue, 12 May 2020 16:58:46 GMT
Server: Apache/2.4.18 (Ubuntu)
[…]
```

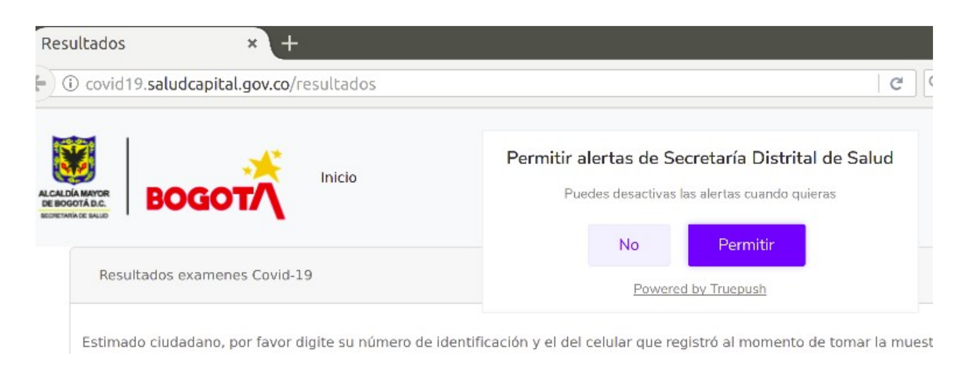
El hecho de entregar de esta manera la versión del servidor no es recomendado ya que puede dar información valiosa a un eventual atacante, esto es aun más problemático en este caso dado que la versión de Apache 2.4.18 tiene varias vulnerabilidades conocidas explotables.



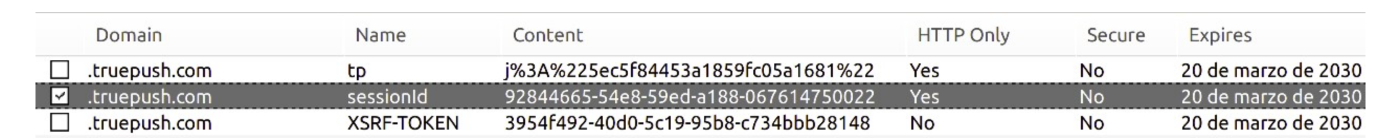


[6] Rastreo por TruePush, incluso en caso de rechazo del servicio

Al llegar en la página de inicio, aparece el siguiente mensaje:



Incluso cuando se hace clic en “No”, las siguientes *cookies* del servicio TruePush se instalan:

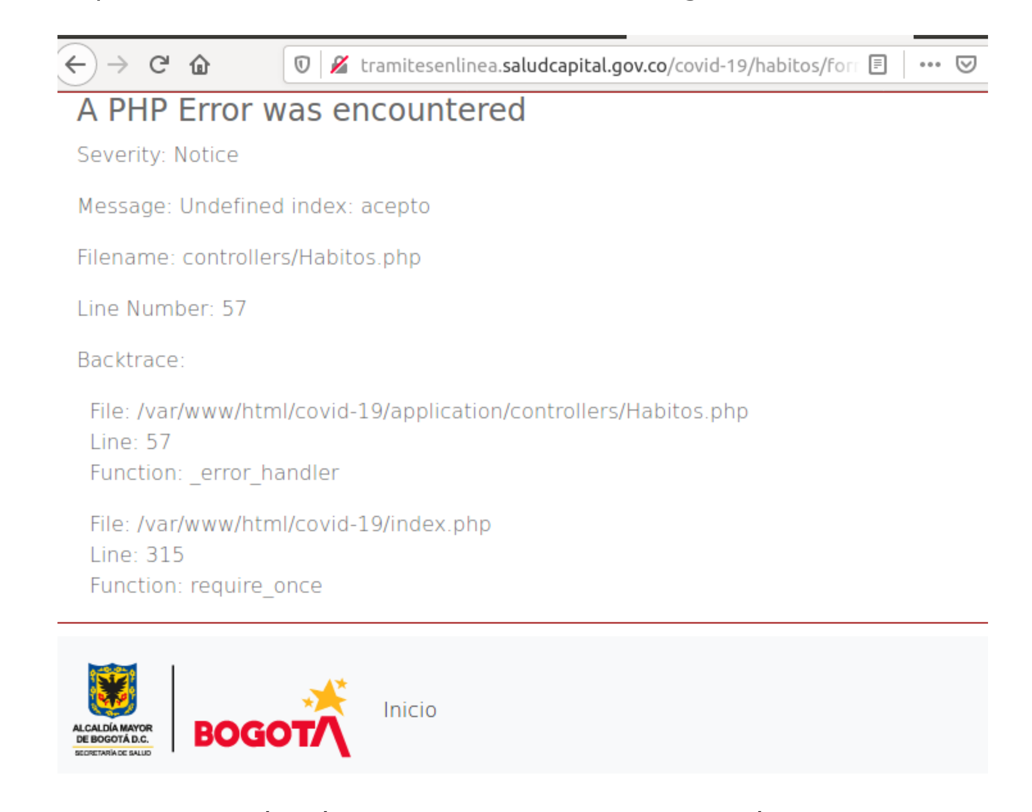


Domain	Name	Content	HTTP Only	Secure	Expires
.truepush.com	tp	j%3A%225ec5f84453a1859fc05a1681%22	Yes	No	20 de marzo de 2030
.truepush.com	sessionId	92844665-54e8-59ed-a188-067614750022	Yes	No	20 de marzo de 2030
.truepush.com	XSRF-TOKEN	3954f492-40d0-5c19-95b8-c734bbb28148	No	No	20 de marzo de 2030

La *cookie* “sessionId” contiene un número único de identificación hexadecimal. A pesar de su nombre no es una *cookie* de sesión sino una cookie de rastreo con una fecha de expiración en 2030.

[7] Divulgación de error de aplicación

En caso de entrar directamente la URL del formulario “Hábitos/Autocuidado” sin pasar por la página anterior (si se entra directamente a la dirección “http://tramitesenlinea.saludcapital.gov.co/covid-19/habitos/formHabitos”), se genera el siguiente error que se muestra directamente en el navegador del usuario:



Este aviso revela información técnica de un error de aplicación y da una mala imagen del sitio web.
Este comportamiento de divulgación de error de aplicación se repite después de los envíos de datos de los formularios, esta vez de manera no visible para el usuario pero entregando muchos más detalles. Esto ocurre en la respuesta del servidor en los POST siguientes:

POST http://tramitesenlinea.saludcapital.gov.co/covid-19/habitos/procesarFormCol

POST http://tramitesenlinea.saludcapital.gov.co/covid-19/habitos/procesarFormInd

El servidor responde con el detalle en una decena de error. Aquí sólo ponemos dos cómo ejemplo:

<h4>A PHP Error was encountered</h4>

<p>Severity: Notice</p>
<p>Message: Undefined index: eps</p>






```
<p>Filename: controllers/Habitos.php</p>
<p>Line Number: 553</p>

    <p>Backtrace:</p>

            <p style="margin-left:10px">
            File: /var/www/html/covid-19/application/controllers/Habitos.php<br />
            Line: 553<br />
            Function: _error_handler                    </p>

            <p style="margin-left:10px">
            File: /var/www/html/covid-19/application/controllers/Habitos.php<br />
            Line: 257<br />
            Function: enviarCorreoAlerta                </p>
```

En todos estos casos se divulgan los errores y la ruta (“path”) de los archivos y carpetas que están en el servidor. Este tipo de información técnica podría ser utilizada por un atacante. Este tipo de vulnerabilidad se llama “Full path disclosure”[22].

[22] https://owasp.org/www-community/attacks/Full_Path_Disclosure





[8] Envio de los datos de registro/movilidad por la aplicación GABO con HTTPS

BOGOTÁCuidadora

Regístrate

* Karisma
Segundo Apellido
* MiContraseña01
* Transversal 22A#59-44
* test@karisma.org.co
* 3505943410
*1985-01-01
5
Aceptar Términos de uso y política de privacidad
ENVIAR CANCELAR

Inicio Rápido | Request & Response
Encabezamiento: Vista Raw | Cuerpo:Vista Raw

```
POST https://api.bogota.gov.co:8246/gabouser/registry/api/v1/user/application/
HTTP/1.1
user: user@user.com
Content-Type: application/json
Content-Length: 370
Connection: Keep-Alive
User-Agent: okhttp/3.12.1
Host: api.bogota.gov.co:8246
```

{"address":"Transversal 22A#59-44","birthdate":"1985-01-01","cellPhone":
"3505943410","email":"test@karisma.org.co","firstLastName":"Karisma",
"firstName":"Fundacion","fullName":"Fundacion Karisma ","identificationNumber
"10123456","identificationType":"CC","middleName":"","password":
"MiContraseÃ±a01","secondLastName":"","stratum":"5","userName":
"test@karisma.org.co"}

Reportar Movilidad

Localidad de residencia:
Chapinero
Hora de Salida:
06:00 PM
Localidad de Destino:
La Candelaria
cra 5#7
Hora de Llegada al destino:

Inicio Rápido | Request & Response
Encabezamiento: Vista Raw | Cuerpo:Vista Raw

```
POST https://api.bogota.gov.co:8246/gabomovility/movility/api/v1/movili
HTTP/1.1
authorization: Bearer bdd6524f-f54b-308f-bf4d-c8ce77155583
Content-Type: application/json
Content-Length: 195
Connection: Keep-Alive
User-Agent: okhttp/3.12.1
Host: api.bogota.gov.co:8246
```

{"checkIn":"07:00 PM","checkOut":"06:00 PM","convenyanceId":5,"desti
"cra 5#7","locationDestination":"La Candelaria","locationOrigin":"Chap
"ocupationId":2,"origin":"","userName":""}

El formulario de reporte del sitio web (Bogota Cuidadora), también se envió con HTTPS, hacia esta URL: https://forms.office.com/formapi/api/f351a7cb-f94a-4df0-9627-ae030ccef7c4/users/fbb08e05-806a-4485-a177-74c90995a2bc/forms('y6dR80r58E2WJ64DDM73xAWOsPtqgIVEoXd0yQmVorxUOE0xN0RKN1UwVE1RT0sxUVpLVUdRMTEzNi4u')/responses





[9] Cookies de rastreo en el formulario de Registro de Movilidad

Al llegar al formulario de registro de movilidad de la plataforma web “Bogota Cuidadora” de la Alcaldía de Bogotá, albergado en Microsoft Forms**,** se instalaron las siguientes *cookies* en nuestro dispositivo:
(URL: https://forms.office.com/Pages/ResponsePage.aspx?id=y6dR80r58E2WJ64DDM73xAWOsPtqglVEoXd0yQmVorxUOE0xN0RKN1UwVE1RT0sxUVpLVUdRMTEzNi4u)

Domain	Name	Content	Expires
.office.com	MUID	3E9DD3B0675A627023DFDD54664E6328	3 de julio de 2021 21:24:32 ...
.c.bing.com	SRM_B	3E9DD3B0675A627023DFDD54664E6328	3 de julio de 2021 21:24:27 ...
.bing.com	MUID	3E9DD3B0675A627023DFDD54664E6328	3 de julio de 2021 21:24:27 ...
forms.office.com	MSFPC	GUID=2b3c3c7994b844d5afcc9f9a31bec967&HASH=2b3c&LV=20...	8 de junio de 2021 21:24:2...
.microsoft.com	MC1	GUID=2b3c3c7994b844d5afcc9f9a31bec967&HASH=2b3c&LV=20...	8 de junio de 2021 21:24:1...
forms.office.com	DcLcid	ui=1033&data=1033	8 de setiembre de 2020 21:...
.c.office.com	MR2	0	15 de junio de 2020 21:24:...
.c.office.com	MR	0	15 de junio de 2020 21:24:...
.c.bing.com	MR2	0	15 de junio de 2020 21:24:...
.c.bing.com	MR	0	15 de junio de 2020 21:24:...
.microsoft.com	MS0	82b5ff72ce6549749c9a220699dd510a	8 de junio de 2020 21:54:1...
.c.office.com	ANONCHK	0	8 de junio de 2020 21:34:3...
.c.office.com	SM	C	At end of session
.forms.office.com	AADNonce.forms	ea9c71ff-2d5f-4c06-926c-c74ed47be0cd.637272662575295819	At end of session
forms.office.com	__RequestVerificationT...	reShKF_QFldnKTqi2zMpFtaFjaLwPs18UPdq7AbSBXgZOhOW3c6...	At end of session

Las 5 primeras tienen todas las características de *cookies* de rastreo: contienen un número de identificación único (hexadecimal) y tienen una duración de vida de más de un año. Están todas asociadas a dominios que pertenecen a Microsoft. Además la finalidad publicitaria de la *cookie* “MUID” esta claramente documentada en el sitio web de la compañia y se usa por su filial publicitaria Microsoft Advertising:

https://about.ads.microsoft.com/en-gb/resources/policies/microsoft-advertising-click-measurement-description-of-methodology





[10] Notificaciones de exposición por medio de anuncios publicitarios en Instagram y Google

Anuncios:









Formularios: [que es el formulario "Alertas" analizado en la parte 2 de este informe]

